Absoluité du conducteur de matrice

Christophe Chalons

Absoluité du conducteur de matrice

Christophe Chalons, université Paris7, équipe de logique mathématique

March 20, 2016

1 Introduction

Le déterminant est probablement l'une des découvertes mathématiques les plus puissantes et les plus fascinantes qui a un nombre complètement incroyable d'applications et qui est à l'origine de nombreux progrès et nombreuses découvertes. C'est probablement l'une, sinon la, des plus spectaculaires conquêtes du raisonnement hypothético-déductif finitiste. J'ignore qui l'a découvert.

2 La puissance quasi-magique du déterminant

Dans cette section, je liste les incroyables propriétés du déterminant. Certaines évoquent dans leur énoncé le mot déterminant, mais surtout, d'autres ne le font pas. Elles donnent ainsi lieu à une blague particulièrement cruelle: à quelqu'un qui ne connait pas le déterminant, vous demandez de prouver l'énoncé (puisque l'énoncé n'utilise pas la notion de déterminant, c'est correct comme devinette). Selon toute vraisemblance, le quelqu'un en question sera plongé dans une galère indicible (à moins qu'il n'ait le génie de réinventer le déterminant). Evidemment, l'intérêt principal du déterminant est de le faire agir dans des anneaux qui possèdent tout plein de diviseurs de 0. Son rôle dans le corps est essentiellement pédagogique (en ce sens que pour ce qui est des corps, ce que donne le déterminant peut être retrouvé relativement facilement sans. Toute proportion gardée évidemment, je ne suis pas un expert ès déterminant)

Tout se passe dans les anneaux commutatifs (parfois unitaires, parfois non). Soit A un tel anneau. Si $M \in M_n(A)$ est une matrice carrée, on dira qu'un élément de l'anneau est produit par M quand il est dans le conducteur de M. Le conducteur de M étant l'ensemble des éléments x de l'anneau tels que $\forall u \in A^n : xu \in Im(M)$

2.1 propriétés avec le mot "déterminant"

Propriété1: le déterminant d'une matrice est productible par la matrice. (Essayez de le prouver, vous allez voir, ça n'a rien de marrant, ni de trivial)

Propriété2: à une multiplication près par (-1) le déterminant d'une matrice ne change pas quand on permute lignes ou colonnes de cette matrice. (Là encore, le prouver demande un certain travail)

Propriété3: celle qui fait la joie des étudiants de premier cycle. Le déterminant ne change pas si on ajoute à une ligne une combinaison linéaire des autres. (Cette propriété permet de calculer vite le déterminant dans un corps. C'est un peu plus problématique dans un anneau).

Jusqu'ici on a listé quelques propriétés calculatoires du déterminant (à part la propriété1), mais pas mentionné sa vraie puissance. Cela est dû au fait que ce sont les propriétés qui précèdent qui vont le rendre puissant (et expliquer pourquoi les énoncés sans le déterminant qui sont des théorèmes sont difficillissimes à prouver sans connaitre le déterminant et ses invariances)

Propriété4: si le déterminant d'une matrice est nul alors la matrice n'est pas injective. **colorred C'EST LA PROPRIETE LA PLUS IMPORTANTE**. Elle entraîne quasiment tout le reste. Elle n'est pas du tout facile à prouver (pour ceux qui connaissent, la comatrice peut tout à fait être nulle et on n'est pas très avancé sauf à faire de lourds calculs). La propriété4 a une corollaire spectaculaire:

Propriété5: si une matrice est injective alors son déterminant est régulier (autrement dit "injectif"). Cette propriété hallucinante est une conséquence triviale de la précédente.

Preuve: soit d le déterminant de M (d'ordre n) et $e \neq 0$ tel que $ed = 0$. Soit $J := \{x \in Anneau \mid ex = 0\}$. Alors $Anneau/J$ voit d comme nul, donc M comme non injective, donc il y a une colonne C telle qu'au moins une des coordonnées de C n'est pas dans J qui vérifie $MC \in J^n$. Alors $eC \neq 0_{Anneau^n}$ et $M(eC) = 0_{Anneau^n}$. CQDFD

Je passe maintenant à la section la plus spectaculaire. Je rappelle au lecteur que les anneaux intègres sont sans intérêt dans l'angle que veut focaliser ce pdf. La plupart des résultats y sont triviaux (un anneau intègre se comporte, dans notre angle, essentiellement comme un corps). Les résultats qui suivent sont en quelque sorte, "logiquement inattendus".

2.2 propriétés SANS le mot "déterminant"

Les propriétés qui suivent sont très faciles à prouver avec le déterminant. Seule la première (numérotée 6) est facile à prouver SANS. Les anneaux sont commutatifs (et on peut les imaginer unitaires, mais c'est peu influent)

Propriété6: une matrice ayant plus de lignes que de colonnes a ses lignes liées. Autrement dit, si $f : A^n \to A^p$ est une application linéaire injective, n, p des entiers alors $p \leq n$ ou $1_{Anneau} = 0_{Anneau}$

Cette première propriété est prouvée dans mon autre pdf, je la copie-colle en appendice. C'est la seule qui semblait accessible à une preuve logique non inspirée (encore qu'il m'a fallu de l'inspiration pour trouver cette preuve, mine de rien). Les propriétés suivantes, qui impliquent la 6 elles, ou bien ont des preuves (sans déterminant) super outillées (noethérianité, etc) que j'ai pu trouvées, ou bien (le plus fréquent) n'avaient pas de preuves simples. Je commence par une propriété rigolote, très parlante (et dont une preuve complexe, mais sans déterminant peut se faire en moins de 3 pages).

Propriété7: toute matrice carrée dont les lignes sont liées a aussi ses colonnes liées (essayez donc de le prouver à partir de rien, vous allez voir la galère!!). La suivante est une conséquence directe du déterminant, mais je ne sais pas la prouver sans (en moins de 40 pages lol). C'est une recopie de la prop5.

Propriété8: une matrice carrée injective produit un élément régulier. (C'est y pas beau??? Donnez cet exo à un matheux, par exemple un américain étudiant, même brillant, en 1er cycle, qui n'a jamais entendu parler de déterminant: succès garanti, vous allez le faire chier d'une force..)

Je rappelle (ou plutôt signale, mais c'est trivial) que l'ensemble des scalaires produits par une matrice est un idéal. Cet idéal contient le déterminant, mais attention, le déterminant n'est pas forcément un générateur de cet idéal. La propriété suivante exploite cet idéal (dont on n'utilise pas le mot déterminant pour le définir)

Propriété9: soit A un anneau et M une matrice carrée dans A. Soit J l'idéal des scalaires produits par M (c'est à dire le conducteur de M). Alors pour tout idéal $K \supset J$, l'anneau A/K voit la matrice M comme étant non injective

Les propriétés suivantes achèvent la liste et ne font que reprendre les précédentes en les incluant dans un constat formel amusant.

Propriété10: Soit A un anneau commutatif unitaire, et M une matrice carrée d'ordre k. Il existe un élément x produit par A et une suite finie $u := (u_1, .., u_f)$ d'éléments de A tels que $u_f = 1$ et pour tout $n \leq f$ tel que $k < n$, il existe une colonne C telle que $MC = (u_{n-1}, u_{n-2}, ..)$ et u_n est une des coordonnées de C, avec en outre que chaque u_i pour $i \leq k$ est dans l'idéal (x)

Propriété11: Soit A un anneau commutatif unitaire, et M une matrice ayant k colonnes et $k-1$ lignes. Il existe une suite finie $u := (u_1, .., u_f)$ d'éléments de A tels que $u_f = 1$ et pour tout $n \leq f$ tel que $k < n$, il existe une colonne C telle que $MC = (u_{n-1}, u_{n-2}, ..)$ et u_n est une des coordonnées de C, avec en outre que chaque u_i pour $i < k$ est nul.

Les propriétés 10 et 11 se ressemblent. La propriété11 est la seule qu'on peut prouver facilement sans déterminant, car elle n'est qu'une traduction de la prop6. La 10, vous l'aurez deviné n'évoque pas (mais y pense) le déterminant. Le x dont l'existence est affirmée est le déterminant de la matrice.

2.3 Propriétés culturelles

Je signale sans la numéroter une propriété absolument spectaculaire du déterminant en ... analyse. En résumé, elle dit que le déterminant permet de prouver le théorème de Brouwer en quelques lignes via la formule de Stokes.

On en trouvera une preuve résumée par exemple au lien : http://www.les-mathematiques.net/phorum/read.php?4,1

3 Questions dont j'ignore la réponse

Un anneau a une propriété particulièrement réduisante: $(A, +)$ est un groupe. C'est particulièrement tueur de généralité dans beaucoup de situations où on a bien deux opérations dont l'une est distributive par rapport à l'autre mais où il ne faut surtout pas qu'il y ait de structure de groupe (sous peine d'obliger tout le monde à être égal).

Un exemple typique est quand $\forall x : x + x = x$. Une telle propriété de la structure entraine que $x = 0$ dès lors qu'on voudrait la plonger dans un groupe. Des opérations distributives les unes par rapport aux autres sont très nombreuses, y compris celles distributives par rapport à elle-même. Soit par exemple $(E, *)$ commutative associative et où $\forall x : x * x = x$ (en gros c'est par exemple l'union, ou l'intersection des ensembles). Alors $*$ est distributive par rapport à $*$. (C'est absolument évident: $a*(b*c) = (a*a)*(b*c) = (a*b)*(a*c)$)

Les deux questions qui suivent semblent donc généraliser de manière assez substantielle ce qui précède à des structures plus générales que des anneaux. Je vais les énoncer sous forme de conjecture. On suppose que E est un ensemble, muni de deux opérations $*, +$ associatives, commutatives et vérifiant $\forall x, y, z$: $x * (y + z) = (x * y) + (x * z)$.

Conjecture1: soit $n > 0$ un entier. Soit f une application linéaire de E^{n+1} dans E^n où linéaire veut dire que $f(x + y) = f(x) + f(y)$ et $f(a * x) = a * f(x)$ pour toutes valeurs des lettres avec x, y dans E^n et

$a \in E$, en ayant défini $(x_1, .., x_n) + (y_1, .., y_n)$ par $(x_1 + y_1, .., x_n + y_n)$ et $a * (x_1, .., x_n) = (ax_1, ax_2, .., ax_n)$. Alors si f est injective alors $card(E) \leq 1$.

Conjecture2: soit $n > 0$ un entier. Soit f une application linéaire de E^n dans E^n. Il existe alors trois éléments ϵ, a, b dans E et deux élément u, v de E^n tels que : $f(u) = (\epsilon, \epsilon, .., \epsilon, a)$ et $f(v) = (\epsilon, \epsilon, .., \epsilon, b)$ et pour tout quotient compatible E' de E, si $a \equiv b$ alors E' voit f comme non injective, ou E' comme ayant un unique élément.

4 Un théorème qui clôt l'affaire

L'énoncé le plus fort est celui dit qu'une matrice carrée à coefficients dans un ACU(:=anneau commutatif unitaire) qui est injective est telle que son conducteur contient un élément régulier. Nous allons, comme il est peu étonnant, prouver un peu plus.

Soit A un anneau tel que $1_A \neq 0_A$, $n > 0$ un entier et $M \in M_n(A)$. Nous dirons que M est superliée quand pour tout idéal J de A, si $1 \notin J$ alors il existe une matrice colonne ayant n lignes C telle que l'une au moins des coordonnées de C n'est pas dans J et telle que MC a toutes ses coordonnées dans J.

Théorème 1 *Soit A un anneau tel que $1_A \neq 0_A$, $n > 0$ un entier et $M \in M_n(A)$. Alors si M n'est pas superliée, il y a dans le conducteur de M un élément régulier*

Ce résultat est assez étonnant car il relie de manière uniforme une propriété calculatoire de l'anneau et **la vie de la matrice dans tous les quotients de l'anneau**

5 Preuve

La preuve du théorème passe par un lemme amusant.

Lemme 2 *Soit A un anneau non trivial, $n > 0$ un entier et $M \in M_n(A)$ dont la première ligne n'est composée que d'éléments nilpotents. Alors M est liée (ie n'est pas injective)*

Preuve: on peut supposer que la première ligne de M contient le moins possible d'éléments non nuls (on minimise ce nombre en parcourant toutes les matrices d'ordre n et **tous les anneaux**). On peut aussi supposer que le premier élément de sa première ligne est non nul, quitte à permuter les colonnes. Appelons-le a et supposons que $a^{k+1} = 0$ et $a^k \neq 0$. Soit $J := \{x \in A_m ida^k x = 0\}$. L'anneau A/J voit la matrice M comme n'ayant que des nilpotents sur la première ligne et un élément nul de plus que M. Il s'ensuit qu'il voit M comme une matrice liée. Soit $C \in A^n \setminus J^n$ tel que $MC \in J^n$. Alors $a^k C \neq 0$ et $M(a^k C) = 0$. La matrice M est liée.

5.1 Preuve du théorème

On considère la collection des triplets (A, n, M) tels que A est un ACU, $n > 0$ un entier et $M \in M_n(A)$ n'est pas superliée et pourtant aussi telle qu'il n'y a pas de matrice colonne C et d'élément régulier $r \in A$ telle que $MC = (0, 0, ..., 0, r)$. On en choisit un tel que n est le plus petit possible. Il existe donc un idéal J ne contenant pas 1 tel que A/J voit M comme injective.

On peut supposer que le premier élément de la première ligne n'a aucune de ses puissances dans J, quitte à permuter les colonnes et grâce au lemme précédent. Notons $(a, b_2, .., b_n) := L_1$ la première ligne de M. On considère la matrice N suivante: sa première colonne est celle de M. Pour $i \geq 2$, sa colonne i est $aC_i - b_iC_1$. On obtient ainsi une matrice $\in M_n(A)$ dont tous les éléments de la première ligne sont nuls sauf le premier. Soit P la matrice obtenue en partant de N et en retirant première ligne et première colonne.

On a donc l'un des deux possibilités suivantes, et rien qu'elles:
1/ ou bien il existe une matrice colonne C ayant $n-1$ lignes telle que PC est de la forme $(0, 0, ..., 0, r)$ avec r régulier
2/ ou bien P est superliée

Dans le premier cas, on a terminé. Il reste donc à analyser le second cas. Soit K l'idéal $\{x \in A \mid \forall n \in \mathbb{N} : a^n x \neq 0\}$. Comme aucun puissance de a n'est dans J, l'idéal K ne contient pas 1. La superliaison de P entraîne l'existence de $(c_2, .., c_n) \notin K^{n-1}$ qui lie les colonnes de P du point de vue de A/K, c'est à dire que $c_2D_2 + .. + c_nD_n \in J^{n-1}$ en notant $D_2, .., D_n$ les colonnes de P.

Cela entraîne que $c_2(aC_2 - b_2C_1) + c_3(aC_3 - b_3C_1) + .. + c_n(aC_n - b_nC_n) = 0 \in J^n$. Soit $i \geq 2$ tel que $c_i \notin K$. alors $c_ia \notin K$, donc en particulier $c_ia \notin J$. Contradiction car on obtient la liaison $(-c_2b_2 - c_3b_3 - .. - c_nb_n).C_1 + c_2aC_2 + .. + c_naC_n \in J^n$ (ie M est liée du point de vue de A/J)

References

[Cha5] C. Chalons, L'effacement du temps par les anneaux commutatifs, article en cours de publication sur HAL (2014).

[Kun] Kunen 1980: Set Theory. Springer verlag

[Pen] Roger Penrose: Les ombres de l'esprit. traduction de Shadows of mind. Paris interedition 1995

[Pra] Pratt every prime has a succint certificate SIAM journal on computing Vol 4 214-252 Theory of ultrafilters. Comfort Negrepontis Springer Verlag 1974

[Cha51] Kaplansky (son Commutative Rings de 1974). Nom : "Regular Element Property" (REP)

[Cha52] Eisenbud (livre) : chap 3, Associated primes and Primary decomposition et le fameux "surprising dichotomy corr. 3.2"

[Cha53] http://www.math.uiuc.edu/ r-ash/ComAlg/ComAlg1.pdf